[2345/115]

DECODER DEVICE FOR DECRYPTING ENCRYPTED TELEVISION PROGRAMS

The invention relates to a decoder device for decrypting encrypted television programs. In particular, the present invention relates to a decoder device having a control unit, for the decryption of encrypted television programs, having an input for feeding in an encrypted television program, a decryption device, which decrypts an encrypted television program into a format that can be reproduced by a television receiver, an output, which can be connected to a television receiver in order to feed the decrypted television program into the television receiver for reproduction, an interface for an identification and/or key carrier component for enabling the decryption device, and an interface for a control unit of the decoder device.

A decoder device of this type enables the reception and decryption of so-called pay TV programs, present-day decoder devices being commercially available as so-called set-top boxes for conventional television receivers.

The invoicing that has been customary heretofore, for example monthly invoicing, for supplying programs in pay TV is shifting more and more to an individual ("pay-per-view") invoicing practice. Therefore, there is a need to identify and authenticate the program customer before the program customer accesses the program. In addition, in the case of so-called HOT programs (home order television), the program customer's orders are also debited to said customer's bank account or his credit on a smart card. Here, too, it is necessary to identify and authenticate the program customer and, when needed, implement security mechanisms to protect against misuse.

To secure electronic invoicing processes, and to protect confidential information (bank account data, account balances, etc.), use is made of smart cards having microprocessors which are equipped with encryption algorithms. An encryption algorithm of this type is the so-called RSA algorithm. In the case of pay TV, a smart card of this type is part of the so-called "conditional access system" (CAS), which is used to check whether the person making the inquiry is actually the authorized program customer and, if applicable, whether his creditworthiness suffices for the desired service. In so-called "electronic commerce", as well, this smart card represents the identity of the customer or of his electronic purse. In this context, a replenishable credit can be recorded on the smart card. The smart card is generally accessed, in a more or less automated manner, by third parties (program providers, commercial entities or the like), via telephone or the internet, using the set-top box before or during the transaction.

A growing problem in this connection is the rising number of program or service providers which a program customer can subscribe to via these media. The result is an ever increasing outlay for equipment (set-top box, television set, internet terminal (PC or net PC), remote control units for the set-top box and the television set, as well as an ever increasing number of smart cards needed to utilize the individual services.

The object of the present invention is, therefore, to design these various components to be less expensive, i.e., to reduce their hardware outlay, and to design them to be less susceptible to faults and simpler for the program customer to handle. Moreover, the present invention intends to consider the problem of security

which is becoming increasingly relevant, in connection with services being utilized by unauthorized third parties.

This objective is achieved in accordance with the present invention by configuring the interface for the identification and/or key carrier component in the control unit of the decoder device.

This design makes it possible to reduce the number of interfaces. Moreover, the program customer (user) is able to carry out his transactions in a more convenient manner, since the control unit of the decoder device is equipped with a keypad in any case. Furthermore, security is improved, since the program customer (even among a relatively large number of third parties) can effect his inputs (PIN, TAN, etc.) without third parties being able to observe this. Moreover, the control unit of the decoder device can be kept securely, together with the identification and/or key carrier component, (smart card), whereas, as a rule, for the sake of convenience, a smart card is not removed from the decoder device (= set-top box).

In accordance with one preferred embodiment of the decoder device having a control unit in accordance with the present invention, the control unit is also set up for controlling the television receiver set, which has an interface for receiving control commands from the control unit. This constitutes a further reduction in equipment outlay. Moreover, overall access to the television receiver set can be controlled. In other words, even television use for programs that do not involve payment must be enabled by the authorized user. This can be achieved by having the function of the control unit as a

whole depend on the authorized user inputting the identifier (PIN).

In order for the program provider to handle debiting and to identify the program customer, in the case of the decoder device according to the present invention, use is made, in particular, of an interface to a telecommunications network. This can be a modem, or a corresponding coupling device for digital telecommunications networks.

In particular, to enhance security in the system, an interface to an identification and/or key carrier component is used. Via such an interface to a telecommunications network, the program customer can make contact with a service provider or merchandise shipper. Here as well, a connection to a specific subscriber (service provider or merchandise shipper) via the telecommunications network is established as a function of an authorization by the identification and/or key carrier component. The program provider is thus considered independently of the service provider or merchandise shipper, when the program customer is invoiced. This can be advantageous with respect to data security and flexibility.

Alternatively, however, it is also possible that the program provider and the service provider cooperate in a suitable fashion, making it possible to have a shared invoicing and/or customer administration, as well as customer identification and customer authorization. In such a case, there is no need for separate smart cards.

At any rate, it is advantageous for the interface to the identification and/or key carrier component for the

authorization of the connection via the telecommunications network to also be arranged in the control unit.

As already mentioned, the identification and/or key carrier component for the authorization of the connection via the telecommunications network and the identification and/or key carrier component for enabling the decryption device can be implemented either by two separate or by one common smart card.

In a further refinement, the decoder device is provided with an interface for connecting the decoder device to a computer, which is set up for controlling the decoder device and/or for establishing a connection to another subscriber via the telecommunications network. It is, thus, possible to make available to the program customer the entire functionality of a computer (PC or internet PC), i.e., the storing and processing of data and information, as well as the more convenient configuration of dialogs between the program customer and, for example, the program provider or the service provider.

In one especially preferred specific embodiment of the present invention, the control unit is formed by the computer, which has an interface for controlling the decoder device, and an interface for the identification and/or key carrier component for authorizing the connection via the telecommunications network and/or the identification and/or key carrier component for enabling the decryption device. This eliminates the need for one or two separate control units. It goes without saying that in this specific embodiment as well, the two smart cards for the traffic with the program provider and the service provider can also be realized as one common smart

card.

It should also be mentioned that the connection between the computer and the television set, or the computer and the decoder device, can either be wire-free (for example, an infrared or ultrasonic connection) or wire-based. In addition, the special demands placed on the computer (relatively small memory, no need for an especially ergonomic keyboard due to mostly short inputs, etc.), mean that a so-called palmtop design is possible, with the appropriate interfaces (infrared interface to the decoding device of one such or more interfaces for the smart card(s)). Thus, the user is able to control and operate his equipment in a very compact and convenient manner, and also simply and conveniently communicate with the program provider and/or the service/merchandise provider. Finally, there is also a substantial reduction in the outlay for cabling between the individual components at the user end, which likewise enhances the convenience.

One especially preferred specific embodiment of the present invention provides for the decoder device to be integrated in the television set. The user is thus provided with a self-contained apparatus which is specially protected against misuse, and in which all of the functions (conventional television, pay TV, communication with a service/merchandise provider via the telecommunications network, storage and/or post-processing of the received data in the computer, etc.) can be performed in a manner in which they are protected from misuse.

The present invention also relates to a smart card for an above-described decoder device with a control unit,

having a computer unit, a first memory area, in which are stored at least parts of operating system functions which are used to control the communication between the computer unit of the smart card and the peripherals of the smart card, as well as the communication with an external host computer, and which are used to manage protected, unprotected and/or read/write memory areas of the smart card, and having a second memory area, which is subdivided into protected and unprotected areas, access to protected areas being made as a function of a check for permitted access, a general key being stored in the protected area of the second memory area, and under the control of the general key, the external host computer entering at least one further simple key, as well as a protocol program associated with this further simple key.

This smart card makes it possible for the decoder device described above to be operated quite securely and also simply, thereby expanding the access to a plurality of additional service providers.

Preferably stored in the second memory area is a key management, from which access is made to a protocol program of a simple key.

In this context, the following method according to the present invention is used to supplement additional keys, i.e., ways of accessing additional providers:

- a telecommunications connection is established by the host computer between the host computer and the decoder device with the control unit or the computer containing the control unit;
- the host computer checks the general key in the smart card;
- a simple key, as well as a protocol program

associated with the key are communicated to the smart card in encrypted form, in the case that the check test has a positive result;

- the simple key and the protocol program associated with the key are entered into the protected memory area of the smart card;
- the protected memory area of the smart card is inhibited.

In this context, before the simple key and the protocol program associated with the key are entered into the protected memory area of the smart card, the key and the protocol program can be decrypted by the computer unit of the smart card.

Figure 1 shows a related-art arrangement in a schematic block diagram.

Figures 2 - 4 depict various specific embodiments of the present invention, each in a schematic block diagram.

Figure 1 illustrates terminal environment for combined pay TV and electronic commerce applications that is customary today. The broadband, digitally encrypted pay TV useful signal is received by the television set via line (1) and transferred via output (4) to input (IN), into set-top box (STB). There, the signal is decrypted by a special chip using an algorithm provided for this - the DVB algorithm is mentioned here as being representative of all such algorithms - and retransmitted to the television set. The keys are set by a smart card (ICC DVB) via interface (3). The smart card contains the key-distribution algorithm of the conditional access system (e.g. RSA) and the customer's secret key. Only a customer having a valid smart card (ICC DVR) is able to decrypt

pay TV broadcasts. The smart card (ICC DVR) is connected to set-top box (STB) via smart card interface "IFD".

Enhancements to set-top box (STB) envisage connecting a backward channel via the telephone network or internet via interface (5) to the servers of various service providers, e.g., for ordering services or goods advertised on the pay TV channels. To safeguard the order and payment, a second smart card (ICC BC) can be inserted in this case via a further interface (IFD), establishing connection (6) between second smart card (ICC BC) and second interface (IFD).

Other possible enhancements for linking set-top box (STB) envisage using an IR remote control (9) and a computer PC via an interface (7) that is customary in the PC environment, referred to here simply as "PCI" (e.g., V24/RS232C or parallel interface). The computer PC facilitates, for example, user-friendly backward channel transactions or the post-processing of information from the pay TV channels.

There are various ways to connect two smart cards to set-top box (STB). Either smart card terminals (IFD) are permanently installed in set-top box (STB), or they are designed to be insertable as PCMCIA modules. PCMCIA modules make it possible to exchange one pay TV access method (CAS) for another without any intervention in set-top box (STB).

Disadvantages associated with conventional terminal configurations include the lack of user-friendliness, the elaborate cabling of set-top box (STB), and its complicated interface configuration.

Specific embodiments of the present invention are illustrated in Figures 2, 3 and 4.

The remote controls of set-top box (STB) and of television set (TV set) are combined in one device, control unit (RCU), already in a first integration stage according to Figure 2. The new control unit (RCU) receives a smart card interface, capable of driving both smart card (ICC DVB) of the pay TV system, as well as smart card (ICC BC) of the backward channel. In terms of the functional sequence, the key exchange of the conditional access system (CAS) of the pay TV is carried out exactly as in the conventional configuration.

In Figure 2, however, an IR interface links smart card (ICC) DVB via control unit (RCU) to the pay TV decryption chip (e.g., DVB) in set-top box (STB). The same applies to smart card (ICC) BC, which, at this point, likewise safeguards the backward channel via control unit (RCU) and its IR interface.

It is, therefore, no longer necessary to insert smart cards into set-top box (STB), eliminating the need for any smart card interfaces at the set-top box (STB). The customer inserts his cards directly into the remote control RCU. If pay TV providers and backward channel service providers agree contractually to this effect, then the functions of both smart cards ICC DVB and ICC BC can even be combined on a single smart card (ICC).

In Figure 2ff, the computer PC either continues to be connected to set-top box (STB) via a conventional interface (PCI) or likewise utilizes the IR interface (infrared interface) of set-top box (STB) for this purpose.

The backward channel connection to the telecommunications network is effected either via set-top box (STB) or via the computer (PC). Both variants are possible in principle.

Figure 3 shows remote control (RCU) and computer (PC) combined in a further integration stage. Here, one can utilize the advantages of the computer PC and of remote control (RCU) simultaneously. This approach is of particular interest when the combined apparatus RCU/PC is similar to a "network PC" and can be operated compactly and without complicated peripherals and cabling, e.g., from the living room table.

Figure 4 illustrates the television set (TV set) and set-top box (STB) combined in just one terminal, as a further integration stage.

The new terminal configurations illustrated in Figures 2 through 4 show how one can appreciably simplify the operation and cabling of the terminals without degrading functionality.

Therefore, in accordance with the present invention, instead of one or more smart card interfaces on the set-top box (STB), the relevant smart cards are now connected via a remote control RCU and its infrared interfaces to the pay TV decryption chip remaining in set-top box (STB). Thus, the need is eliminated for costly and delicate interfaces on the set-top box (STB).

Moreover, the functions of the pay TV smart card and of the backward-channel smart card can be combined in a user-friendly manner on just one card, with the assistance of a special remote control RCU.

Finally, combining the remote control and the PC in just one apparatus RCU/PC makes it possible to move the backward channel connection out of the set-top box (STB). This makes it possible to optimally utilize the internet PC (= PC which is linked via any desired online networks to servers of any desired service providers), in conjunction with pay TV services, including their backward channel options.

A further aspect of the present invention is configuring the smart card so that it, too, can handle, with a high level of security, both the decryption of the program of the pay TV provider and transactions (ordering and payment of purchase price) with the goods/service provider.

In particular, if further goods/service providers are added over time, this means in each case that the program customer needs a new smart card containing the keys and protocols of the previous providers (both pay TV providers and goods/service providers) and the key and the protocol of the newly added provider.

The present invention likewise provides an approach for this:
Since the goods/service provider is linked in any case, as a rule, to the user by the same host computer as the pay TV provider, this host can also access the inhibited areas of the customer's smart card by a general key, in order to store there a further key and the associated protocol for future transactions (decryption or payment processes).

Moreover, a vector table or an interrogation routine, in which the newly added keys are successively managed, is

to be executed in an additional area (possibly likewise inhibited). In response to a smart card access, it is first checked on the basis of the vector table or the interrogation routine to see whether an appropriate key is present, or whether the key input by the user matches one of the keys stored on the smart card. Only when this interrogation has a positive result, is the program associated with the respective key (if indicated, decrypted and then) executed for the purpose of transaction or decryption.

The key and the associated protocol (program) are preferably likewise transmitted in an encrypted form, from the host computer to the box (STB) and, from there, routed via the interface to control unit (RCU). When control unit (RCU) is integrated in computer (PC/RCU), the host computer can be directly linked to computer (PC/RCU) via the telecommunications network, to transmit the information for the, i.e., into smart card (ICC).

Depending on the specific configuration, it is possible for the protocol (program) to be stored in the smart card just in an encrypted form, and for it to be decrypted in each case for the delay prior to execution. Alternatively, however, the protocol (program) can also be rendered in an executable form when it is stored in the (protected) memory area of the smart card.

As a result, the memory of the smart card contains (inter alia) the following programs and/or data:

An operating system core for controlling communications between the smart card processor and the peripherals on the smart card, as well as communications with the host computer which manages the memory areas of the smart card

(protected and unprotected areas, read/write areas, flash EEPROM, etc.), etc. Keys (a master or general key, and also one or more application keys), the master key being used to transfer (further) application keys and the associated application or protocol programs into the memory area. The application keys ensure that the protocol programs are executed (and thus orders handled or pay TV programs decrypted) only in response to proper user input.

Encrypted user programs or protocol programs for controlling the handling of orders or the decryption of pay TV programs.

To enhance security, provision is made for the identification and authentication between the control unit (RCU) and/or the set-top box (STB) or television set (TV set), on the one hand, and the host computer, on the other hand, to be carried out on different routes or channels. In other words, some of the protocol traffic is transmitted via interface (5) to the telephone network, and some via line (1), together with or prior to the broadband, digitally encrypted pay TV useful signal. In this context, the enabling/inhibiting of services can also take place on these routes. Since a case of misuse would require synchronously intercepting and decrypting both channels, security is thus considerably higher. In particular, information can be distributed between the two channels at the time of enabling/inhibiting, or of new keys, etc., in such a way that it is able to be decrypted only in an alternating and also only in a step-by-step manner, in each instance, with knowledge thereof.